FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005-3315

202 • 408 • 4000
FACSIMILE 202 • 408 • 4400

ATLANTA
404•653•6400
PALO ALTO
650•849•6600

WRITER'S DIRECT DIAL NUMBER:

TOKYO
011•813•3431•6943
BRUSSELS
011•322•646•0353

jc685 U.S. PTO
02/07/00

(202) 408-4024

February 7, 2000

ATTORNEY DOCKET NO.: 04284.0829

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

New U.S. Patent Application
Title: PORTABLE ELECTRONIC DEVICE AND A METHOD FOR ISSUING THE DEVICE
Inventor: Takafumi WATANABE

Sir:

We enclose the following papers for filing in the United States Patent and Trademark Office in connection with the above patent application.

1. A check for $730 representing a $690 filing fee and $40 for recording the Assignment.

2. Application - 19 pages, including 3 independent claims and 17 claims total.

3. Drawings - 5 sheets of drawings, containing 13 figures.

4. Declaration and Power of Attorney.

5. Recordation Form Cover Sheet and Assignment to Kabushiki Kaisha Toshiba .

Applicant claims the right to priority based on Japanese Application No. 11-029976, filed February 8, 1999.

Please accord this application a serial number and filing date and record and return the Assignment to the undersigned.

09496995 "020700

The Commissioner is hereby authorized to charge any additional filing fees due and any other fees due under 37 C.F.R. § 1.16 or § 1.17 during the pendency of this application to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By: _____
Richard V. Burgujian
Reg. No. 31,744
ERNEST F. CHAPMAN
Reg. No. 25,961

RVB/FPD/dvz
Enclosures

09490895 - 020700

Attorney Docket No.04284-0829

UNITED STATES PATENT APPLICATION

TAKAFUMI WATANABE

FOR

PORTABLE ELECTRONIC DEVICE AND A METHOD FOR ISSUING THE DEVICE

09460965 - 052707

BACKGROUND OF THE INVENTION

I. Field of the Invention

The present invention generally relates to a portable electronic device, and a method for issuing the device. More particularly, the present invention relates to a device and method for achieving high security during application operation and high efficiency while being issued.

II. Background and Material Information

A portable electronic device such as an IC card prevents an unauthorized third person from reading and rewriting data stored in an internal memory, writing new data into the internal memory by a security function realized by, such as, a personal identification number (PIN) code, and encoding data to be transmitted to or from a card reader/writer.

An IC card needs to be written with specific data necessary for operation of each application. For example, an IC card may require entry of an owner's PIN code and cryptographic key for an application so that the IC card can become usable for the application. This process of writing the specific data into the IC card is called "issuance." An issuer usually issues a large number of IC cards with specific data at a time. Each issued IC card requires satisfaction of the security function except for the owner's PIN code. Therefore, because a preparatory process such as a data encoding process must occur before the issuing process, this preparatory process makes issuing the card inefficient.

Therefore, demanded is a mechanism in which (1) an unissued IC card can be written with the specific data without satisfying with the

security function and (2) the security function becomes valid after the issuance and each IC card requires satisfaction of the security function in case of data writing or data rewriting. That is, an IC card with which achieves high security during application operation and high efficiency during issuance is demanded.

SUMMARY OF THE INVENTION

In view of the foregoing, the present invention solves the inherent limitations of existing issuing systems by use of a specific application program and a method for issuing the device that substantially obviates one or more of the problems due to limitations and disadvantages of the past approaches.

In accordance with an aspect of the present invention, as embodied and broadly described, the present invention is directed to a portable electronic device. The device comprises means for executing a security function against unauthorized use, the security function is validated by a command received from outside the device, means for storing data necessary to use the application program, and means for storing data indicating whether the security function is valid based on the command.

Also in accordance with another aspect of the present invention, there is provided a portable electronic device. The device comprises a nonvolatile memory, means for storing validity data indicating whether the security function is valid into the nonvolatile memory, wherein the validity data is received as a command message from the outside of the device, first means for determining whether a command message provided from outside the device includes data for the security function,

second means for determining whether the nonvolatile memory is stored with the validity data, and first means for writing or rewriting data into the nonvolatile memory following the command message, when the first determining means determines the command message does not to include the data for security function, and, wherein the second determining means determines the nonvolatile memory not to be stored with the validity data.

In accordance with another aspect of the present invention, there is provided a method for issuing a portable electronic device. The method comprises providing a security function against unauthorized use into the device, storing in the device data necessary to use the application program, and validating the security function by issuing a command after storing said data. The security function is validated by the command received from outside the device.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed. Further features and/or variations may be provided in addition to those set forth herein. For example, the present invention may be directed to various combinations and subcombinations of the disclosed features and/or combinations and subcombinations of several further features disclosed below in the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate various embodiments

and/or features of the invention and together with the description, serve to explain the principles of the invention. In the drawings:

FIG.1 is an exemplary block diagram depicting the configuration of an IC card processing apparatus 100 according to the principles of the present invention;

FIG. 2 is an exemplary block diagram depicting the function of IC card 102;

FIG. 3 is an exemplary block diagram depicting the configuration of IC module 300;

FIG. 4 is a diagram depicting a mapping example in data memory 304 after the issuance;

FIG. 5 is a diagram depicting an example of DF definition information;

FIG. 6 is a diagram depicting an example of EF definition information generated subordinately to a DF definition information;

FIGs. 7(a)-(d) are diagrams depicting writing or rewriting command message format examples;

FIG. 8 is a diagram depicting a message format example of a command that validates security flag 510;

FIG. 9 is an exemplary flowchart depicting a process for validating security flag 510 of the DF definition information; and

FIG. 10 is an exemplary flowchart depicting a process generated by a command message for writing or rewriting.

DETAILED DESCRIPTION

The various aspects and features of the present invention will be

hereinafter described with reference to the accompanying drawings.

FIG.1 is an exemplary block diagram depicting the configuration of an IC card processing apparatus 100 according to the principles of the present invention. IC card processing apparatus 100 communicates with an IC card 102. IC card processing apparatus 100 comprises a computer 104 which generally controls IC card processing apparatus 100. IC card 102 and computer 104 communicate with each other using a card reader/writer 106. For example, IC card 102 and computer 104 may be physically connected, or not physically connected, such as an antenna. IC card processing apparatus also comprises a keyboard 108 for inputting a command and data, a cathode ray tube (CRT) display 110 for displaying data, a printer 112 for printing data, and a floppy disk drive (FDD) 114 for storing data, all of which are connected to computer 106.

FIG. 2 is an exemplary block diagram depicting the function of IC card 102.

IC card 102 comprises a reading/writing unit 200, a PIN setting/collating unit 202, an encoding/decoding unit 204, and a supervisor 206. Supervisor 206 controls various functions executed by units 200, 202, and 204.

The functions of units 200, 202, and 204 are now further described. Reading/writing unit 200 reads data from and writes data into a data memory 302 (further described below) and a program memory 304 (further described below) with specific commands or specific data provided by computer 104 via card reader/writer 106.

PIN setting/collating unit 202 sets an owner's PIN code in data

memory 302 when an IC card is issued, replaces the PIN code when requested by the owner, and collates a PIN code provided by computer 104 in comparison with the set PIN code when the IC card is used.

Encoding/decoding unit 204 encodes data provided by IC card 102 to computer 104, and decodes encoded data provided from computer 104 to IC card 102.

Supervisor 206 receives a command (and data) from card reader/writer 106, interprets that command, and instructs units 200, 202, and 204 to execute various functions, such as read, write, encode, or decode.

FIG. 3 is an exemplary block diagram depicting the configuration of IC module 300.

IC module 300 comprises a CPU 302, a data memory 304, a program memory 306, and a contact unit 308. CPU 302 controls IC module 300. Data memory 304 is a nonvolatile memory for storing various data, such as an EEPROM. Program memory 306 is a mask ROM printed a control program. A mask ROM is a ROM chip printed with data for a program when produced. Contact unit 308 is an interface between IC 310 and card reader/writer 106.

An IC 310 contains CPU 302, data memory 304, and program memory 306. IC module 300 is composed of contact unit 308 and IC 310 connected with contact unit 308. IC card 102 is formed with IC module 300 and a plastic card (not shown) for packing IC module 300.

FIG. 4 is a diagram depicting a mapping example in data memory 304 after the issuance.

Data memory 304 comprises a system area 400, a dedicated file (DF) / elementary file (EF) definition area 402, and a data area 404.

System area 400 stores fixed data and initial value of variable data, both of which are necessary to use IC card 102. Both data are stored in system area 400 before the issuance.

DF/EF definition area 402 stores both DF definition information and EF definition information. DF definition information defines an application, and EF definition information defines data to be used for the application. In FIG. 4, two pieces of EF definition information, EF1-1 and EF1-2, are given respective EF identifiers "EF1" and "EF2." The information is stored in DE/EF definition information area 402 correspondingly to DF definition information named "DF1."

DF/EF definition area 402 also comprises an unused area for storing DF definition information and EF definition information. This information is added when IC card 102 is additionally issued regarding a new application, or when new data is additionally written into a current application.

Data area 404 stores data and CPU 302 manages the stored data using EF definition information. Data area 404 also stores one or more programs for each application. Each application is managed on the basis of DF definition information so that validity or invalidity of the security function of an application can be set separately among applications.

FIG. 5 is a diagram depicting an example of DF definition information.

DF definition information comprises a DF name 500, DF size

information 502, security format information 504, and a security flag 506. Every DF has a unique DF name 500 by which CPU 302 looks up a corresponding DF. DF size information 502 is an area in data memory 304 which both a DF and EFs subordinate to the DF can use. When a new EF is added subordinately to a DF, the size of the new EF is subtracted from the size stored in DF size information. Security format information 504 stores information regarding message formats of writing or rewriting commands to be executed under a DF.

Security flag 506 is set while security of an application is valid. When security flag 506 is set, only a writing or a rewriting command having the same message format as designated by corresponding security format information 504 is accepted, however, writing or rewriting command having other format will be refused, and not accepted.

FIG. 6 is a diagram depicting an example of EF definition information generated subordinately to a DF definition information.

EF definition information comprises DF information 600, an EF identifier 602, address information 604, EF size information 606, and EF format information 608.

DF information 600 indicates a dominant DF to an EF. Every EF has a unique EF identifier 602 by which control element 302 looks up a corresponding EF. Address information 604 stores an address in a data area managed on the basis of a corresponding EF definition information. EF size information 606 indicates the size of a data area managed on the basis of a corresponding EF definition information. EF format information 608 stores information regarding the structure of an EF

definition information. An international organization for standardization (ISO) provides a record structure EF and a transparent structure EF in ISO7816-4. More information on ISO7816-4 may be found in: International Organization for Standardization, "International Standard ISO/IEC 7816: Integrated circuit(s) cards with contacts."

FIGs. 7(a)-(d) are diagrams depicting a writing or rewriting command message format examples.

As shown in FIG. 7(a), a format #1 is a basic command of writing or rewriting. The format #1 comprises a command header area and data area. The command header indicates whether the command is a writing command or a rewriting command. The data area comprises data to be written or rewritten to data memory 304. The format #1 is accepted when security flag 506 is not valid.

On the other hand, formats #2-#4 respectively shown in FIG. 7(b)-(d) are accepted when security flag 506 is valid.

As shown in FIG. 7(b), a format #2 comprises encoded data area to conceal data. In this case, security verification is carried out through decoding of the encoded data.

As shown in FIG. 7(c), a format #3 comprises a spare data area to realize justifiability of data. In this case, security verification is carried out by determining the justifiability of the spare data.

As shown in FIG. 7(d), a format #4 comprises an encoded data area, and spare data area to realize concealment and justifiability of data. In this case, security verification is carried out judging from encoding results and justifiability of the spare data.

The formats #2-#4 are designated correspondingly to each DF by security format information 504.

FIG. 8 is a diagram depicting a message format example of a command that validates security flag 510.

The command is composed of single command header area. Immediately after an execution of the command, security flag 510 of the DF definition information is validated.

FIG. 9 is an exemplary flowchart depicting process for validating security flag 510 of the DF definition information.

Computer 104 sends a command message to CPU 302 via card reader/writer 106 and contact unit 306 to validate security flag 510 (shown in FIG. 6). Next, CPU 302 receives the command message (step S1). CPU 302 collates the format type of the command message. That is, CPU 302 determines whether the received command message is a command message for validating security flag 510 (step S2). When CPU 302 determines that the command message is a command message to validate security flag 510, CPU 302 validates security flag 510 which is included in a DF definition information under a current processing, hereinafter referred to 'current DF' (step S3).

FIG. 10 is an exemplary flowchart depicting a process generated by a command message for writing or rewriting.

Computer 104 sends a command message for writing or rewriting (shown in FIG. 7(a)-(d)) to CPU 302 via card reader/writer 108 and contact unit 306. Next, CPU 302 receives the command message (step T1). CPU 302 collates the format type of the command message. CPU 302

then determines whether the type of the command message is the format #1 type (step T2). If the message is format #1, CPU 302 determines whether security flag 510 regarding a current DF definition information is validated (step T3). When the security flag 510 is determined not yet to be validated, CPU 302 writes or rewrites as designated by command header area 800 (step T4).

Therefore, an unissued IC card can be written or rewritten with data for application operation without satisfying the security function and accordingly issuance becomes highly efficient.

When the security flag 510 is determined to be already validated in step T3, CPU 302 sends a reply status indicating "the format type of the received command message is not acceptable." to computer 104 (step T5). Thus format #1 will be refused when security flag 510 is validated.

When CPU 302 determines the format type of command message not to be the format #1 (step T2), CPU 302 writes or rewrites data designated by security format information 504 in the current DF definition information using received command message (step T6).

CPU 302 then determines whether the command message can pass the verification by the security function (step T7). When the command message passes the verification, CPU 302 writes or rewrites data designated in command header area (step T4).

When the command message can not pass the verification, CPU 302 sends a replying status indicating "the received command message is not acceptable" to computer 104 (step T8).

As described above, consistent with the principles of the present

invention, an unissued IC card can be written with the specific data without satisfying with the security function and the security function becomes valid after the issuance and each IC card requires satisfaction of the security function in case of data writing or data rewriting. That is, a mechanism in which an IC card with which achieves high security during application operation and high efficiency during issuance.

Other embodiments of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the present invention being indicated by the following claims.

Docket: 56656-650

WHAT IS CLAIMED IS:

1. A method for issuing a portable electronic device containing an application program, comprising the steps of:

providing a security function against unauthorized use into the device, wherein the security function is validated by a command received from outside the device;

storing in the device data necessary to use the application program; and

validating the security function by issuing the command after storing said data.

2. The method of claim 1, wherein storing said data includes the step of:

storing a PIN code used to identify the owner of the device.

3. The method of claim 1, wherein:

said providing a security function comprises providing a plurality of security functions different from each other depending on corresponding application programs; and

said storing data comprises storing a cryptographic key used to identify a corresponding application program.

4. A portable electronic device containing an application program, comprising:

means for executing a security function against unauthorized use, the security function is validated by a command received from outside the device;

means for storing data necessary to use the application program; and

means for storing data indicating whether the security function is valid based on the command.

5. The device of claim 4, wherein:

said data necessary to use the application program is a PIN code used to identify the owner of the device.

6. The device of claim 4, wherein:

said security function executing means executes a plurality of security functions different from each other depending on corresponding application programs; and

said data necessary to use the application program is a cryptographic key to identify a corresponding application program.

7. The device of claim 4, wherein:

said portable electronic device is an IC card.

8. A portable electronic device with a security function, containing an application program, comprising:

a nonvolatile memory;

means for storing validity data indicating whether the security function is valid into the nonvolatile memory, wherein the validity data is received as a command message from the outside of the device;

first means for determining whether a command message provided from outside the device includes data for the security function;

second means for determining whether the nonvolatile memory is stored with the validity data; and

first means for writing or rewriting data into the nonvolatile memory following the command message, when the first determining means determines the command message does not include the data for security function, and, wherein the second determining means determines the nonvolatile memory not to be stored with the validity data.

9. The device of claim 8, further comprising:

first means for outputting a status indicating that the command message is not acceptable, when the first determining means determines the command message not to be including the data for security function, besides, when the second determining means determines the nonvolatile memory to be stored with the validity data.

10. The device of claim 8, further comprising:

third means for determining whether verification of the data for the security function succeeds, when the first determining means determines the command message to be including data for the security function; and

second means for writing or rewriting data into the nonvolatile memory following the command message, when the third determining means determines the verification is successful.

11. The device of claim 9, further comprising:

second means for outputting a status indicating that the command message is not acceptable when the third determining means determines the verification of the data for the security function is not successful.

12. The device of claim 9 wherein the command message comprises:

a writing or rewriting command;

data to be written or rewritten into the nonvolatile memory; and

additional data guaranteeing the justifiability of the data based on verification of the data.

13. The device of claim 9 wherein the command message comprises:

a writing or rewriting command; and

encoded data to be written or rewritten into the nonvolatile memory after being decoded, based on verification of the data.

14. The device of claim 9 wherein the command message comprises:

a writing or rewriting command;

encoded data to be written or rewritten into the nonvolatile memory after being decoded;

additional data guaranteeing the justifiability of the data; and wherein:

the verification of the data is performed based on the encoded data and the additional data.

15. The device of claim 9, wherein the nonvolatile memory stores a plurality of security programs different from each other depending on a corresponding application program.

16. The device of claim 13, wherein each security program is separately validated in response to a prescribed command message for validation, and wherein each security program corresponds to an application program.

17. The device of claim 13, wherein at least one available format of the command message is separately defined, and wherein each format corresponds to an application program.

ABSTRACT OF THE DISCLOSURE

A portable electronic device with which an owner of the device makes use of a specific application program and a method for issuing the device. An unissued IC card can be written with the specific data without satisfying the security function of the IC card. After the issuance of the IC card, the security function becomes valid and each IC card requires satisfaction of the security function in case of data writing or data rewriting.

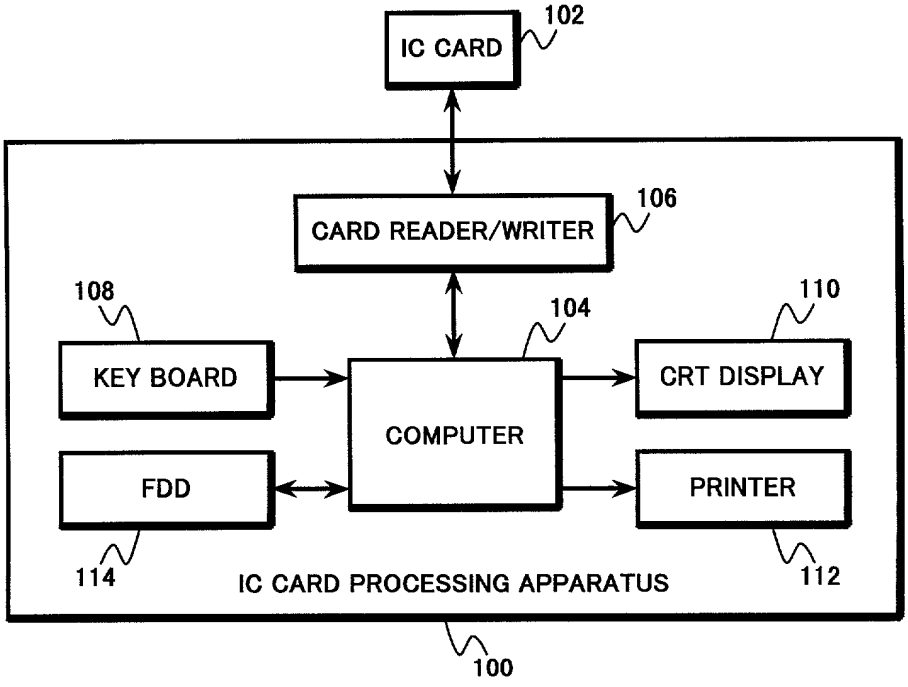
IC CARD
102
CARD READER/WRITER
106
108
104
110
KEY BOARD
COMPUTER
CRT DISPLAY
FDD
PRINTER
114
IC CARD PROCESSING APPARATUS
112
100

FIG. 1

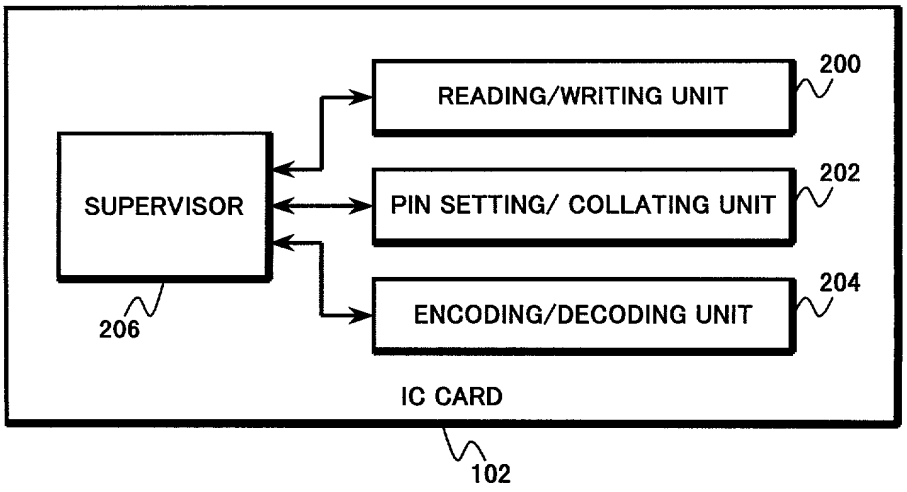
READING/WRITING UNIT
200
SUPERVISOR
PIN SETTING/ COLLATING UNIT
202
ENCODING/DECODING UNIT
204
206
IC CARD
102

FIG. 2

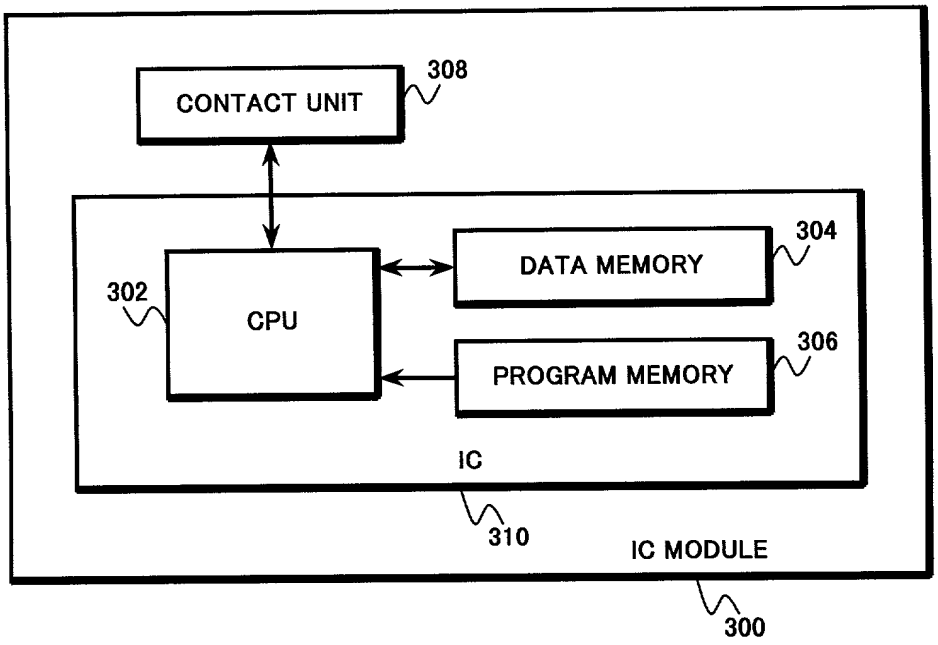
CONTACT UNIT
308
DATA MEMORY
304
302
CPU
PROGRAM MEMORY
306
IC
310
IC MODULE
300

FIG. 3

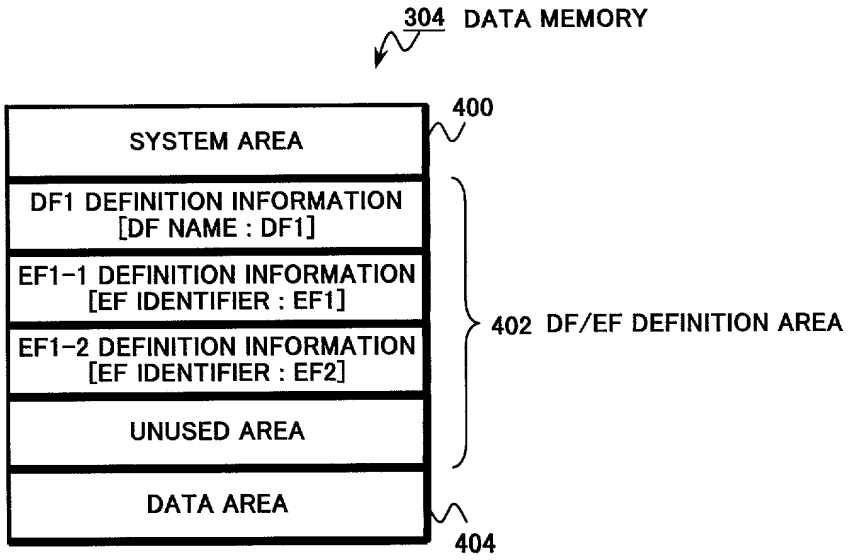
304 DATA MEMORY
400
SYSTEM AREA
DF1 DEFINITION INFORMATION
[DF NAME : DF1]
EF1-1 DEFINITION INFORMATION
[EF IDENTIFIER : EF1]
EF1-2 DEFINITION INFORMATION
[EF IDENTIFIER : EF2]
UNUSED AREA
402 DF/EF DEFINITION AREA
DATA AREA
404

FIG. 4

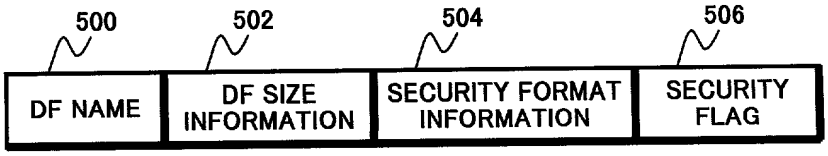

FIG. 5

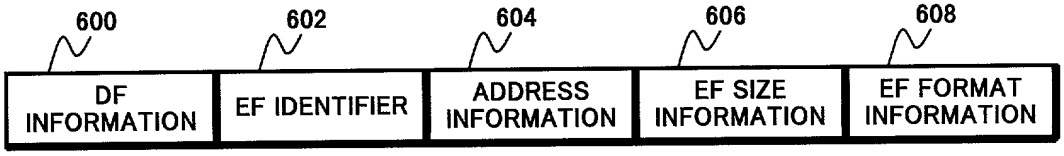

FIG. 6

FIG. 7(a)

FIG. 7(b)

FIG. 7(c)

FIG. 7(d)

COMMAND HEADER

FIG. 8

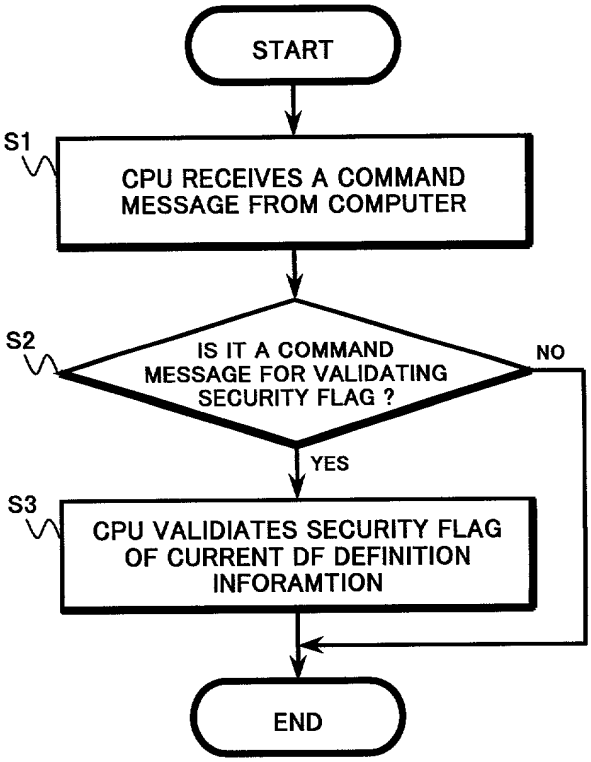
START
S1
CPU RECEIVES A COMMAND MESSAGE FROM COMPUTER
S2
IS IT A COMMAND MESSAGE FOR VALIDATING SECURITY FLAG ?
NO
YES
S3
CPU VALIDIATES SECURITY FLAG OF CURRENT DF DEFINITION INFORAMTION
END

FIG. 9

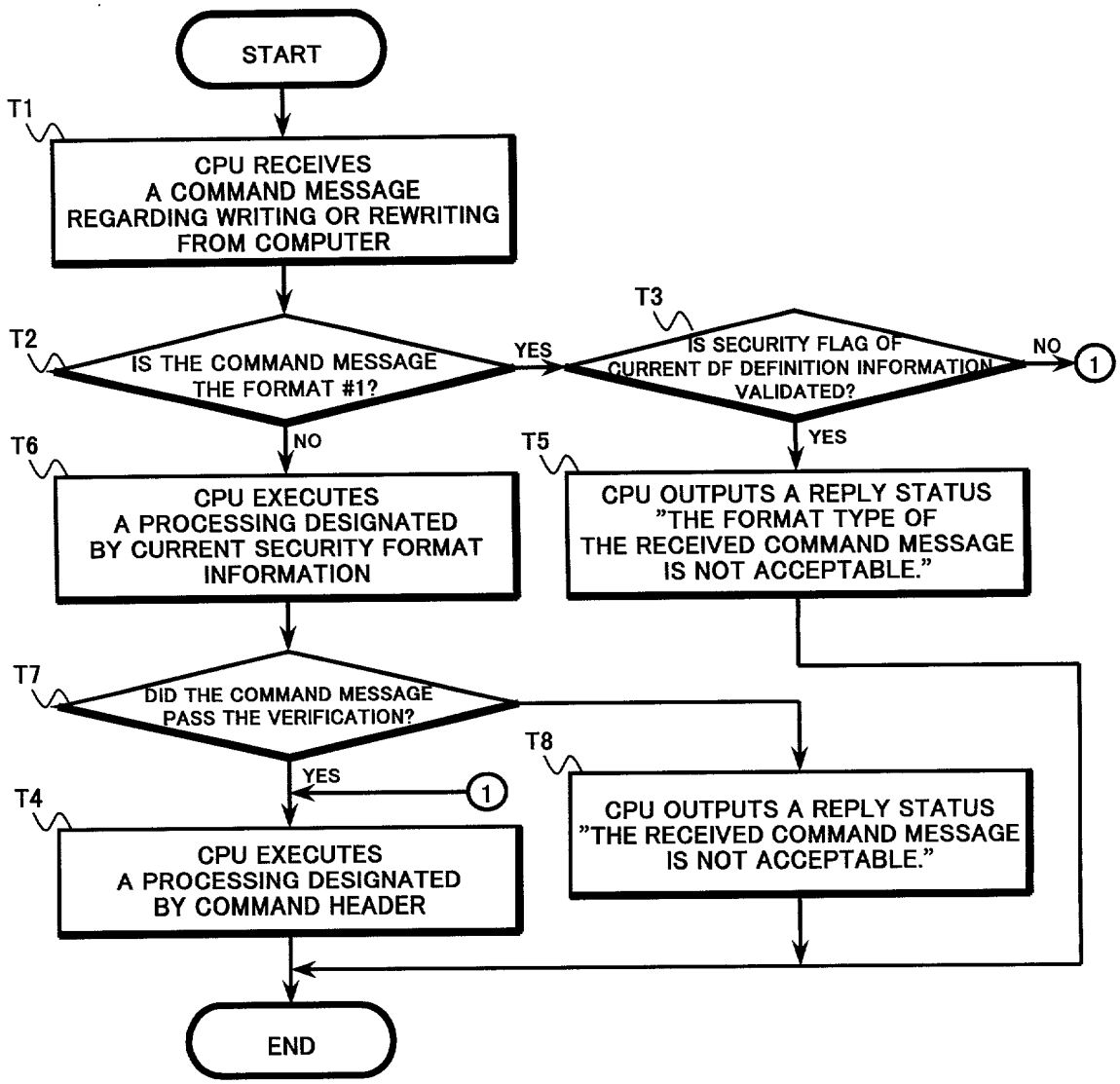
START
T1
CPU RECEIVES A COMMAND MESSAGE REGARDING WRITING OR REWRITING FROM COMPUTER
T2
IS THE COMMAND MESSAGE THE FORMAT #1?
YES
T3
IS SECURITY FLAG OF CURRENT DF DEFINITION INFORMATION VALIDATED?
NO
1
NO
YES
T6
CPU EXECUTES A PROCESSING DESIGNATED BY CURRENT SECURITY FORMAT INFORMATION
T5
CPU OUTPUTS A REPLY STATUS "THE FORMAT TYPE OF THE RECEIVED COMMAND MESSAGE IS NOT ACCEPTABLE."
T7
DID THE COMMAND MESSAGE PASS THE VERIFICATION?
T8
YES
1
T4
CPU EXECUTES A PROCESSING DESIGNATED BY COMMAND HEADER
CPU OUTPUTS A REPLY STATUS "THE RECEIVED COMMAND MESSAGE IS NOT ACCEPTABLE."
END

FIG. 10

Attorney Docket No.:04284.0829

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that: My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

PORTABLE ELECTRONIC DEVICE AND A METHOD FOR ISSUING THE DEVICE

the specification of which:

is attached hereto; or

was filed as United States Application Serial No._____ on _____, and was amended on _____ (if applicable); or

was filed as PCT International Application Number _____ on _____and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate or § 365(a) of any PCT international application(s), designating at least one country other than the United States, listed below and have also identified below any foreign application(s) for patent or inventor's certificate, or any PCT international application(s) having a filing date before that of the application(s) of which priority is claimed:

Country	Application Number	Date of Filing	Priority Claimed Under 35 U.S.C. 119
Japan	11-029976	February 8, 1999	x YES ☐ NO
			☐ YES ☐ NO

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

Application Number	Date of Filing

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s) or § 365(c) of any PCT international application(s) designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application(s) in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Attorney Docket No.:04284.0829

Application Number	Date of Filing	Status (Patented, Pending, Abandoned)

I hereby appoint the following attorney and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. **FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P., Reg. No. 22,540**, Douglas B. Henderson, Reg. No. 20,291; Ford F. Farabow, Jr., Reg. No. 20,630; Arthur S. Garrett, Reg. No. 20,338; Donald R. Dunner, Reg. No. 19,073; Brian G. Brunsvold, Reg. No. 22,593; Tipton D. Jennings IV, Reg. No. 20,645; Jerry D. Voight, Reg. No. 23,020; Laurance R. Hefter, Reg. No. 20,827; Kenneth E. Payne, Reg. No. 23,098; Herbert H. Mintz, Reg. No. 26,681; C. Larry O'Rourke, Reg. No. 26,014; Albert J. Santorelli, Reg. No. 22,610; Michael C. Elmer, Reg. No. 25,857; Richard H. Smith, Reg. No. 20,609; Stephen L. Peterson, Reg. No. 26,325; John M. Romary, Reg. No. 26,331; Bruce C. Zotter, Reg. No. 27,680; Dennis P. O'Reilley, Reg. No. 27,932; Allen M. Sokal, Reg. No. 26,695; Robert D. Bajefsky, Reg. No. 25,387; Richard L. Stroup, Reg. No. 28,478; David W. Hill, Reg. No. 28,220; Thomas L. Irving, Reg. No. 28,619; Charles E. Lipsey, Reg. No. 28,165; Thomas W. Winland, Reg. No. 27,605; Basil J. Lewris, Reg. No. 28,818; Martin I. Fuchs, Reg. No. 28,508; E. Robert Yoches, Reg. No. 30,120; Barry W. Graham, Reg. No. 29,924; Susan Haberman Griffen, Reg. No. 30,907; Richard B. Racine, Reg. No. 30,415; Thomas H. Jenkins, Reg. No. 30,857; Robert E. Converse, Jr., Reg. No. 27,432; Clair X. Mullen, Jr., Reg. No. 20,348; Christopher P. Foley, Reg. No. 31,354; John C. Paul, Reg. No. 30,413; David M. Kelly, Reg. No. 30,953; Kenneth J. Meyers, Reg. No. 25,146; Carol P. Einaudi, Reg. No. 32,220; Walter Y. Boyd, Jr., Reg. No. 31,738; Steven M. Anzalone, Reg. No. 32,095; Jean B. Fordis, Reg. No. 32,984; Barbara C. McCurdy, Reg. No. 32,120; James K. Hammond, Reg. No. 31,964; Richard V. Burgujian, Reg. No. 31,744; J. Michael Jakes, Reg. No. 32,824; Dirk D. Thomas, Reg. No. 32,600; Thomas W. Banks, Reg. No. 32,719; Christopher P. Isaac, Reg. No. 32,816; Bryan C. Diner, Reg. No. 32,409; M. Paul Barker, Reg. No. 32,013; Andrew Chanho Sonu, Reg. No. 33,457; David S. Forman, Reg. No. 33,694; Vincent P. Kovalick, Reg. No. 32,867; James W. Edmondson, Reg. No. 33,871; Michael R. McGurk, Reg. No. 32,045; Joann M. Neth, Reg. No. 36,363; Gerson S. Panitch, Reg. No. 33,751; Cheri M. Taylor, Reg. No. 33,216; Charles E. Van Horn, Reg. No. 40,266; and Linda A. Wadler, Reg. No. 33,218; Jeffrey A. Berkowitz, Reg. No. 36,743; Michael R. Kelly, Reg. No. 33,821; James B. Monroe, Reg. No. 33,971; and _____. Please address all correspondence to **FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.**, 1300 I Street, N.W., Washington, D.C. 20005, Telephone No. (202) 408-4000.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Attorney Docket No.:04284.0829

Full Name of first Inventor Takafumi WATANABE	Inventor's Signature Takafumi Watanabe	Date Jan. 31. 2000
Residence Tokyo, Japan		Country of Citizenship Japan
Post Office Address c/o Intellectual Property Division Toshiba Corporation, 1-1-1, Shibaura, Minato-ku, Tokyo, Japan		

09/769,569